BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

KOREAN PATENT ABSTRACT (KR)

PUBLICATION

(51) IPC Code: H04L 12/22
(11) Publication No.: 2003-0039731 (43) Publication Date: May 22, 2003
(21) Application No.: 10-2001-0070765 (22) Application Date: November 14, 2001

(71) Applicant:
Electronics and Telecommunications Research Institute
161 Gajeong-Dong, Yuseong-Gu, Daejeon 305-350, Korea

(72) Inventor:
LEE, SU HYUNG

LEE, SEUNG MIN

JI, JEONG HOON

OH, SEUNG HEE

NAM, TAEK YONG

(54) Title of the Invention:
Attacker Traceback Method Using Session Information Management Based on Code Mobility

Abstract:

The present invention is an attacker trace back method for identifying the host in which a hacker is actually residing by tracing the hacker's connection when detecting the hacker's direct attack on the host. The prior art was able to protect the domain in which the host was located but was not able to identify the attacker. Therefore the attacker was able to launch a second or third attack on the same host via a host connected to a network that is different from the network that the attacker used in previous attacks. In this case the domain in which the certain host belongs to cannot take any measures against the attacks. Using a session information management system that applies code mobility the present invention traces the locations of the attackers that launch a cyber attack via other hosts on the Internet. Thus, a more effective, active network security is realized.

Tracing the location of the attacker and taking adequate measures against the attacker can prevent a second or third attack by the same attacker.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
H04L 12/22

(11) 공개번호 특2003-0039732
(43) 공개일자 2003년05월22일

(21) 출원번호 10-2001-0070766
(22) 출원일자 2001년11월14일

(71) 출원인 한국전자통신연구원
대한민국
305-350
대전 유성구 가정동 161번지

(72) 발명자 이승민
대한민국
306-777
대전광역시대덕구송촌동461-1선비마을아파트301-502

남택용
대한민국
305-707
대전광역시유성구신성동160-1한울아파트106-604

이수형
대한민국
305-721
대전광역시유성구신성동153하나아파트108-505

지정훈
대한민국
138-796
서울특별시송파구잠실6동장미아파트3차1-802

오승희
대한민국
305-350
대전광역시유성구가정동236-1ETRI기숙사1동328

(74) 대리인 장성구
김원준

(77) 심사청구 있음

(54) 출원명 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역추적 방법

요약

본 발명은 인터넷 환경의 글로벌 네트워크(global network) 차원에서 특정 데이터나 시스템, 서비스의 해킹(hacking)에 대하여 이를 추적하기 위한 공격자 역 추적 방법에 관한 것이다. 종래에는 침입에 대한 로그정보의 기록방법과 형식이 호스트마다 다르기 때문에, 해커의 공격 경로를 수작업으로 분석할 수밖에 없다. 특히, 해커가 자신의 IP(Internet Protocol) 주소를 속여서 공격해 오는 경우에는 호스트에서 남긴 로그정보만으로 해커를 추적하는 것은 불가능하다. 본 발명은, 해커가 자신의 IP 주소를 속여 여러 네트워크를 경유해서 사이버 공격 예로, 서비스를 마비시키는 서비스거부공격(Denial Of Service : DOS) 등을 행할 경우 해커가 존재하는 네트워크의 위치를 추적하도록 한다. 따라서, 특정 기업이나 정부 부처 혹은 국가 차원에서, 국내외 해커로부터 사이버 공격에 효과적으로 대처할 수 있기 때문에, 안전하고 신뢰성 있는 인터넷환경을 보장할 수 있다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법을 실시하기 위한 네트워크 구성도,

도 2는 본 발명에 따른 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법의 일 실시예를 단계별로 나타낸 순서도,

도 3은 도 1에 도시된 에지 라우터에서 기록하는 패킷로그의 일부에 이용되는 IP 데이터그램을 나타낸 도면.

<도면의 주요부분에 대한 부호의 설명>

101 : 공격 호스트 102, 103, 104, 105, 106 : 에지 라우터

107 : 침입 호스트 108 : 침입탐지 시스템

109, 110, 111 : 관리서버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 인터넷(internet)에서 에지 라우터(edge router)의 로그정보(log information)를 이용한 공격자 역 추적 방법에 관한 것으로, 특히, 인터넷 환경의 글로벌 네트워크(global network) 차원에서 특정 데이터나 시스템, 서비스의 해킹(hacking)에 대하여 이를 추적하기 위한 공격자 역 추적 방법에 관한 것이다.

종래에는 외부 네트워크로부터 내부 네트워크로의 공격자 침입에 대하여 경유 호스트(host) 측에서 로그정보를 기록하도록 했다가 이후에 이를 분석하여 해커(hacker)의 공격 경로를 추적하였다.

그러나, 침입에 대한 로그정보의 기록방법과 형식이 호스트마다 다르기 때문에, 해커의 공격 경로를 수작업으로 분석할 수밖에 없다. 특히, 해커가 자신의 IP(Internet Protocol) 주소를 속여서 공격해 오는 경우에는 호스트에서 남긴 로그정보만으로 해커를 추적하는 것은 불가능하다.

발명이 이루고자 하는 기술적 과제

본 발명은 상술한 문제점을 해결하기 위하여 안출한 것으로, 글로벌 네트워크 환경에서 각각의 네트워크의 에지 라우터에서 내부로 접근하는 모든 패킷에 대한 로그정보를 기록하도록 해서 공격자의 IP 주소 변경에 관계없이 해당 패킷에 대한 역 추적을 가능하게 하는 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법을 제공하는 데 그 목적이 있다.

이와 같은 목적을 달성하기 위한 본 발명은, 다수의 상대 네트워크와 선택적으로 각각 연결하는 다수의 에지 라우터, 다수의 호스트, 관리서버, 침입탐지 시스템을 각각 구비한 다수의 네트워크로 이루어지는 통신 시스템에 있어서, 내부의 특정 에지 라우터가 외부 네트워크로부터 내부 네트워크로 들어오는 패킷에 대한 로그정보를 기록하는 제 1 단계; 및 내부의 침입탐지 시스템으로부터 해킹이 감지되는 경우 내부 에지 라우터의 로그정보를 바탕으로 해커의 위치를 역 추적하는 제 2 단계를 포함하는 것을 특징으로 한다.

발명의 구성 및 작용

도 1은 본 발명에 따른 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법을 실시하기 위한 네트워크 구성도로, 에지 라우터(102, 103)에 의해 공격자 로컬 인터넷과 인터넷 서비스 사업자 망이 연결되고 에지 라우터(105, 106)에 의해 침입자 로컬 인터넷과 인터넷 서비스 사업자 망이 연결되도록 구성된다. 상기 침입자 로컬 인터넷, 인터넷 서비스 사업자 망 및 공격자 로컬 인터넷에는 공격자를 추적하기 위한 관리서버(109, 110, 111)가 각각 존재한다. 또한, 상기 침입자 로컬 인터넷, 인터넷 서비스 사업자 망 및 공격자 로컬 인터넷에는 각각 다수의 호스트 및 특정 침입탐지 시스템(Intrusion Detection System : IDS)이 구성되어 있으나 도 1에는 본 발명의 동작 설명에 필요한 호스트 및 침입탐지 시스템만 도시된다.

동 도면에 있어서, 외부의 해커는 자신의 공격 호스트(101)에서 IP 주소를 속여 자신의 에지 라우터(102)와 ISP 도메인(Internet Service Provider domain)(인터넷 서비스 사업자 망)의 에지 라우터(103, 105)를 경유한 후, 침입 도메인(침입자 로컬 인터넷)의 에지 라우터(106)를 통해 침입 호스트(107)를 공격한다. 이 과정에서 각 도메인의 에지 라우터(103, 106)는 외부 도메인으로부터 접근하는 패킷에 대한 로그정보를 기록한다.

침입탐지 시스템(108)은 상기 공격자의 침입을 탐지할 경우 침입정보를 관리서버(109)에게 보고한다.

관리서버(109)는 침입탐지 시스템(108)으로부터 침입정보를 전달받아 에지 라우터(106)의 로그정보를 바탕으로 해커가 위치한 공격자 도메인의 공격 호스트(101)를 추적한다.

도 2는 본 발명에 따른 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법의 일 실시예를 단계별로 나타낸 순서도이다.

먼저, 내부의 침입탐지 시스템(108)은 공격자가 침입 호스트(107)를 공격할 경우 공격자의 침입을 감지한다(단계 201).

내부의 침입탐지 시스템(108)은 내부 네트워크의 관리서버(109)에게 공격자의 침입 사실을 알린다(단계 202).

내부의 관리서버(109)는 내부 네트워크의 모든 에지 라우터(106)에게 내부 네트워크의 침입탐지 시스템(108)으로부터 전달받은 공격자 패킷의 흔적에 대응하는 침입탐지 로그분석을 질의한다(단계 203).

내부의 관리서버(109)는 침입 흔적이 발견되었는지 여부를 내부의 에지 라우터(106)를 통해 판단한다(단계 204).

내부의 관리서버(109)는 단계 204의 판단 결과, 침입 흔적이 발견되면 외부 네트워크로부터의 침입으로 판단하여 침입 흔적에 대응하는 타 네트워크의 관리서버(110)에게 자신의 관리 하에 있는 에지 라우터(103, 104, 105)에게 로그분석을 요청해 줄 것을 의뢰한다(단계 205). 반면, 내부의 관리서버(109)는 단계 204의 판단 결과, 침입 흔적이 발견되지 않으면 내부 네트워크에서의 침입으로 판단하여 내부 네트워크에 해커가 존재하는 것으로 판단한다(단계 208).

타 네트워크의 관리서버(110)는 자신의 관리 하에 있는 에지 라우터(103, 104, 105)에게 로그분석을 요청한다(단계 206).

타 네트워크 관리 하의 에지 라우터(103, 104, 105)가 침입 흔적을 발견했는지 여부를 판단한다(단계 207).

타 네트워크 관리 하의 에지 라우터(103, 104, 105)가 침입 흔적을 발견하는 경우 또 다른 외부 네트워크로부터의 침입이기 때문에, 상기 단계 205부터 상기 단계 207까지 수행하는 과정을 공격자 호스트(101)를 찾을 때까지 되풀이한다. 반면, 타 네트워크 관리 하의 에지 라우터(103, 104, 105)가 침입 흔적을 발견하지 못하는 경우 타 네트워크에서의 침입으로 판단하여 타 네트워크에 해커가 존재하는 것으로 판단한다(단계 208).

여기서, 도메인과 네트워크는 동일한 영역을 의미한다.

도 3은 도 1에 도시된 에지 라우터에서 기록하는 패킷로그의 일부에 이용되는 IP 데이터그램을 나타낸 도면이다.

동 도면에 있어서, 소스 IP 주소(source IP address)(301), 목적 IP 주소(destination IP address)(302), 프로토콜(protocol) 및 서비스 타입(service type)이 패킷로그에 포함된다. 로그정보에는 상기의 네 가지 정보와 패킷이 들어온 에지 라우터의 입력 인터페이스(input interface) 및 에지 라우터를 통과한 시간이 함께 기록된다.

이밖에 버전(version), 헤더 길이(header length), 총 길이(total length), 식별자(identification), 플랙(flags), 프래그먼테이션 오프셋(fragmentation offset), 타임 투 리브(time to live), 헤더 체크섬(header checksum) 및 옵션(option) 등의 항목이 더 있다.

상기와 같은 로그파일은 컴퓨터로 읽을 수 있는 기록 매체에 기록되고, 컴퓨터에 의하여 처리될 수 있다.

발명의 효과

본 발명은, 해커가 자신의 IP 주소를 속여 여러 네트워크를 경유해서 사이버 공격 예로, 서비스를 마비시키는 서비스거부공격(Denial Of Service : DOS) 등을 행할 경우 해커가 존재하는 네트워크의 위치를 추적하도록 한다. 따라서, 특정 기업이나 정부 부처 혹은 국가 차원에서, 국내외 해커로부터 사이버 공격에 효과적으로 대처할 수 있기 때문에, 안전하고 신뢰성 있는 인터넷환경을 보장할 수 있다.

(57) 청구의 범위

청구항 1.
다수의 상대 네트워크와 선택적으로 각각 연결하는 다수의 에지 라우터, 다수의 호스트, 관리서버, 침입탐지 시스템을 각각 구비한 다수의 네트워크로 이루어지는 통신 시스템에 있어서,

내부 네트워크의 침입탐지 시스템이 공격자가 침입 호스트를 공격할 경우 공격자의 침입을 감지하는 제 1 단계;

상기 내부 네트워크의 침입탐지 시스템이 내부 네트워크의 관리서버에게 공격자의 침입 사실을 알리는 제 2 단계;

상기 내부 네트워크의 관리서버가 내부 네트워크의 모든 에지 라우터에게 상기 내부 네트워크의 침입탐지 시스템으로부터 전달받은 공격자 패킷의 흔적에 대응하는 침입탐지 로그분석을 질의하는 제 3 단계;

상기 내부 네트워크의 관리서버가 침입 흔적이 발견되었는지 여부를 상기 내부 네트워크의 에지 라우터를 통해 판단하는 제 4 단계;

상기 내부 네트워크의 관리서버가 상기 제 4 단계의 판단 결과, 침입 흔적이 발견되면 외부 네트워크로부터의 침입으로 판단하여 침입 흔적에 대응하는 타 네트워크의 관리서버에게 자신의 관리 하에 있는 에지 라우터에게 로그분석을 요청해 줄 것을 의뢰하는 제 5 단계;

상기 타 네트워크의 관리서버가 자신의 관리 하에 있는 에지 라우터에게 로그분석을 요청하는 제 6 단계;

상기 타 네트워크의 관리 하의 에지 라우터가 침입 흔적을 발견했는지 여부를 판단하는 제 7 단계;

상기 타 네트워크 관리 하의 에지 라우터가 침입 흔적을 발견하는 경우 또 다른 외부 네트워크로부터의 침입이기 때문에, 상기 제 5 단계부터 상기 제 7 단계까지 수행하는 과정을 공격자 호스트를 찾을 때까지 되풀이하는 제 8 단계를 포함하는 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법.

청구항 2.
제 1 항에 있어서, 상기 내부 네트워크의 관리서버가 상기 제 4 단계의 판단 결과, 침입 흔적이 발견되지 않으면 내부 네트워크에서의 침입으로 판단하여 내부 네트워크에 해커가 존재하는 것으로 판단하는 단계를 더 포함하는 것을 특징으로 하는 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법.

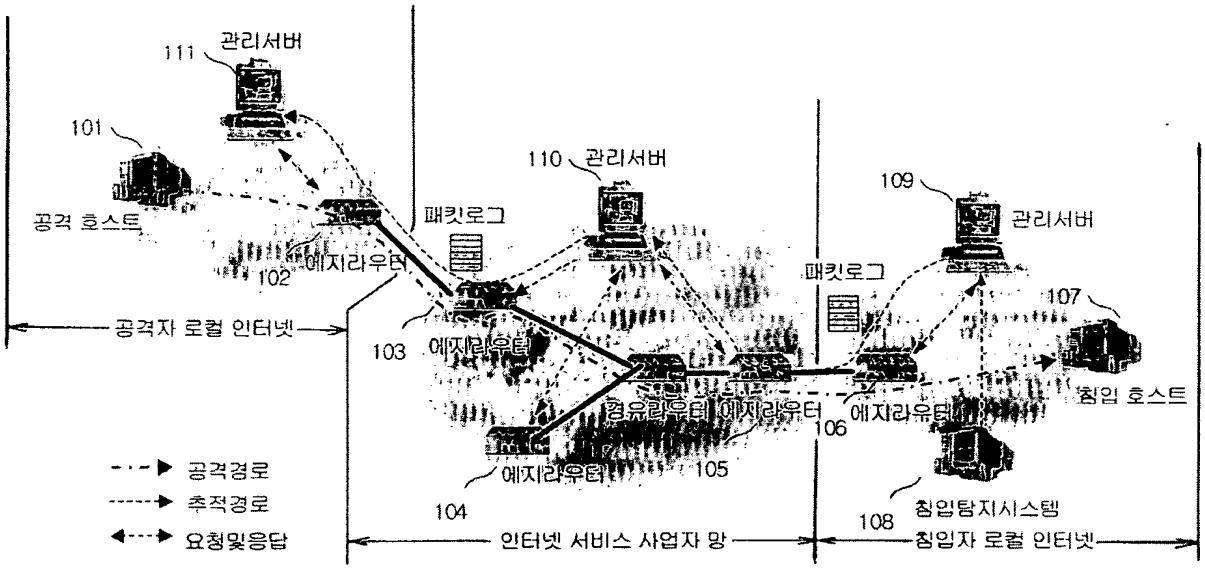
청구항 3.
제 1 항에 있어서, 상기 타 네트워크 관리 하의 에지 라우터가 침입 흔적을 발견하지 못하는 경우 상기 타 네트워크에서의 침입으로 판단하여 상기 타 네트워크에 해커가 존재하는 것으로 판단하는 단계를 더 포함하는 것을 특징으로 하는 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법.

청구항 4.
제 1 항 내지 제 3 항 중 적어도 어느 한 항에 있어서, 상기 로그정보는 외부 네트워크로부터 내부 네트워크로 접근하는 패킷에 대한 정보인 것을 특징으로 하는 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법.

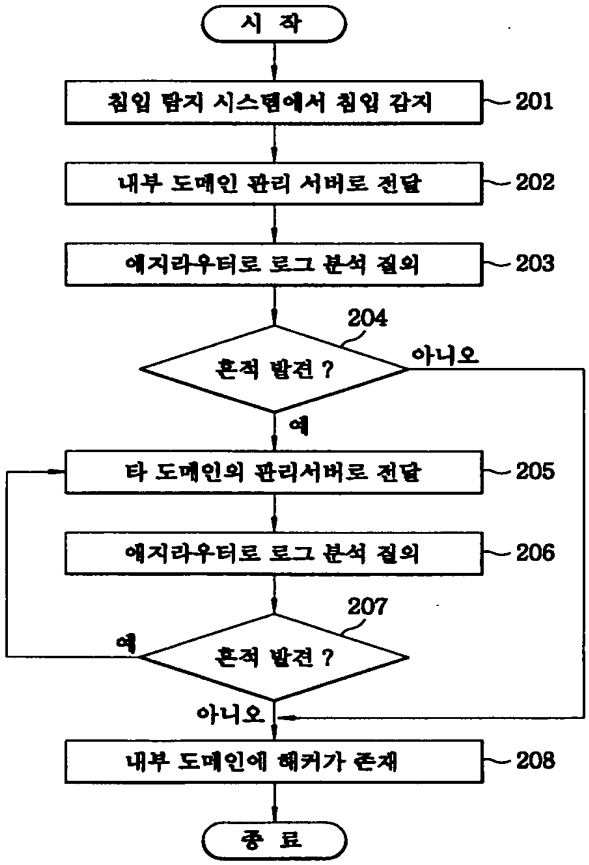
청구항 5.
제 1 항 내지 제 3 항 중 적어도 어느 한 항에 있어서, 상기 로그정보는 소스 IP 주소, 목적 IP 주소, 프로토콜, 서비스 타입, 패킷이 들어온 라우터의 입력 인터페이스 및 에지 라우터를 통과한 시간을 포함하는 것을 특징으로 하는 인터넷에서 에지 라우터의 로그정보를 이용한 공격자 역 추적 방법.

도면

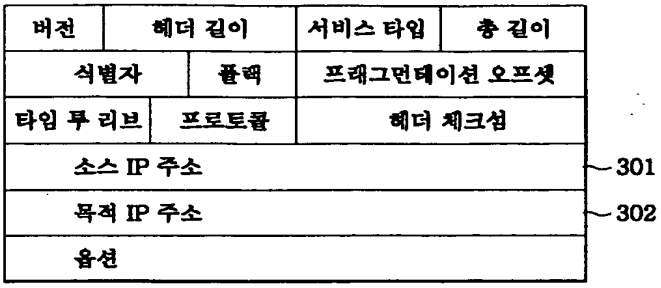
도면 1


111 관리서버
101
공격 호스트
패킷로그
102 에지라우터
110 관리서버
109
관리서버
패킷로그
107
공격자 로컬 인터넷
103 에지라우터
경유라우터
에지라우터
에지라우터
106
침입 호스트
에지라우터
105
104
108 침입탐지시스템
공격경로
추적경로
요청및응답
인터넷 서비스 사업자 망
침입자 로컬 인터넷

도면 2


시 작
침입 탐지 시스템에서 침입 감지
201
내부 도메인 관리 서버로 전달
202
에지라우터로 로그 분석 질의
203
204
흔적 발견 ?
아니오
예
타 도메인의 관리서버로 전달
205
에지라우터로 로그 분석 질의
206
207
예
흔적 발견 ?
아니오
내부 도메인에 해커가 존재
208
종 료

도면 3


버전
헤더 길이
서비스 타입
총 길이
식별자
플랙
프래그먼테이션 오프셋
타임 투 리브
프로토콜
헤더 체크섬
소스 IP 주소
301
목적 IP 주소
302
옵션